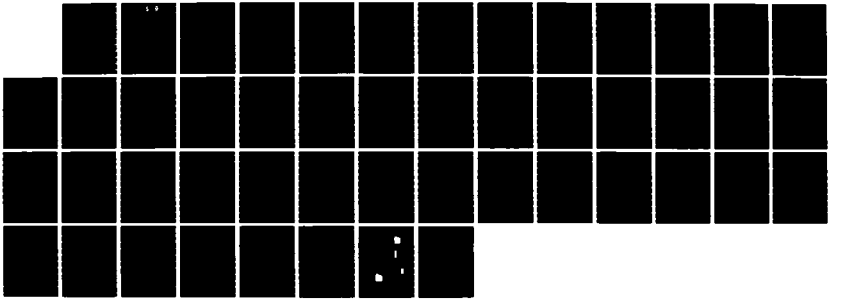
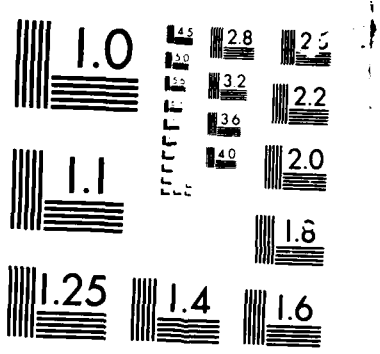
AD-A168 561 APPROXIMATE EVALUATION OF RELIABILITY AND AVAILABILITY VIA PERTURBATION A. (U) MASSACHUSETTS INST OF TECH CAMBRIDGE DEPT OF AERONAUTICS AND A.. 1/1

UNCLASSIFIED B K WALKER ET AL. SEP 85 AFOSR-TR-86-0314 F/G 9/3 NL




1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.8
3.2
3.6
4.0

UNCLASSIFIED

SECURI

DTIC ELECTE JUN 09 1986 S D

T DOCUMENTATION PAGE

1a. RE Ur

AD-A168 561

1b. RESTRICTIVE MARKINGS

2a. SE

3. DISTRIBUTION/AVAILABILITY OF REPORT
Approved for public release; distribution unlimited.

2b. DECLASSIFICATION/DOWNGRADING SCHEDULE
Unlimited

4. PERFORMING ORGANIZATION REPORT NUMBER(S)

5. MONITORING ORGANIZATION REPORT NUMBER(S)
AFOSR-TR- 86-0314

6a. NAME OF PERFORMING ORGANIZATION
Dept. of Aero. & Astro.
Mass. Inst. of Tech.

6b. OFFICE SYMBOL (If applicable)

7a. NAME OF MONITORING ORGANIZATION
Air Force Office of Scientific Research

6c. ADDRESS (City, State and ZIP Code)
77 Massachusetts Ave. - Rm. 33-105
Cambridge, MA 02139

7b. ADDRESS (City, State and ZIP Code)
AFOSR/NM, Building 410
Bolling AFB, DC 20332

8a. NAME OF FUNDING/SPONSORING ORGANIZATION

8b. OFFICE SYMBOL (If applicable)

9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
AFOSR 84-0160

8c. ADDRESS (City, State and ZIP Code)

10. SOURCE OF FUNDING NOS.

PROGRAM ELEMENT NO.	PROJECT NO.	TASK NO.	WORK UNIT NO.
61102F	2304	K3	

11. TITLE (Include Security Classification)
(see other side) Unclassified

12. PERSONAL AUTHOR(S)
Bruce K. Walker, Siu-Kwong Chu and Norman M. Wereley

13a. TYPE OF REPORT Annual

13b. TIME COVERED FROM 6/1/84 TO 5/31/85

14. DATE OF REPORT (Yr., Mo., Day)
September, 1985

15. PAGE COUNT
44

16. SUPPLEMENTARY NOTATION

17 COSATI CODES		
FIELD	GROUP	SUB. GR

18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
Reliability, availability, Markov models

19. ABSTRACT (Continue on reverse if necessary and identify by block number)

Progress is described on a project whose goal is the development of practical tools for evaluating the reliability and availability of fault-tolerant control or sensor systems. The approach relies on the generation of a Markovian model for the behavior of the system in terms of failures and Redundancy Management decisions. The project entails the investigation of approximate techniques for deriving results from these models. The basic idea is that the time-behavior of the model decomposes into two time scales where the results of interest occur in time frames intermediate to the two time scales. By modifying previous theory, an approximate evaluation scheme is developed and shown to be valid for a number of example cases. Ongoing work is also described.

DTIC FILE COPY

86 6 6 046

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT
UNCLASSIFIED/UNLIMITED ☒ SAME AS RPT ☐ DTIC USERS ☐

21 ABSTRACT SECURITY CLASSIFICATION
Unclassified

22a. NAME OF RESPONSIBLE INDIVIDUAL
Maj. Woodruff

22b. TELEPHONE NUMBER (Include Area Code)
(202) 767-5027

22c. OFFICE SYMBOL
NM

DD FORM 1473, 83 APR EDITION OF 1 JAN 73 IS OBSOLETE.

Uncl
SECURITY CLASSIFICATION OF THIS PAGE

11. TITLE: Approximate Evaluation of Reliability and Availability Via Perturbation Analysis

DISCLAIMER NOTICE

THIS DOCUMENT IS BEST QUALITY PRACTICABLE. THE COPY FURNISHED TO DTIC CONTAINED A SIGNIFICANT NUMBER OF PAGES WHICH DO NOT REPRODUCE LEGIBLY.

Annual Progress Report on

Grant AFOSR-84-0160:

Approximate Evaluation of Reliability and Availability Via Perturbation Analysis

Prof. Bruce K. Walker
Siu-Kwong Chu
Norman M. Wereley

Dept. of Aeronautics & Astronautics
Massachusetts Institute of Technology
77 Massachusetts Avenue
Cambridge, MA 02139

September, 1985

Prepared for:
Maj. Brian W. Woodruff
AFOSR/NM
Building 410
Bolling AFB, DC 20332

I. Introduction

The goal of the research is to apply analytical approximation techniques to the problem of practically evaluating fault-tolerant control system reliability and availability where the system behavior is modelled by a finite state Markov or semi-Markov process. The key property of fault-tolerant control systems to be exploited is that component failures tend to occur very infrequently relative to decisions by the redundancy management (RM) system, which include false detection alarms, detections of faults, identification of faulty components and rejection of false alarms. This property tends to cause the resulting Markovian model to exhibit behavior in two (or more) distinct time scales: a fast time scale for the RM decisions and a slow time scale for the component failures. Of interest for reliability and availability studies is usually the behavior that occurs over durations intermediate to the two time scales. Under certain conditions, this behavior can be approximated by an aggregated model whose aggregated state classes reflect primarily the number of component failures. Therefore, the RM decision behavior is considered to have reached steady state instantaneously in the time scale of interest. The advantage of an aggregated model is that it includes only a fraction of the number of states in the original model. It is therefore much more amenable to practical computation than the original model, which is computationally intractable even for simple systems.

The approach to developing simplified models is based primarily on the approximate aggregation theory developed in [1,2]. The primary result from this development is summarized by the following theorem:

Theorem: Given a perturbed finite-state semi-Markov process $z^{\epsilon}(t)$ whose transition operator elements $P^{\epsilon}_{ij}(t)$ have the following dependence on ϵ:

$$P^{\epsilon}_{ij}(t) = (p_{ij} - \epsilon q_{ij})h_{ij}(t/\epsilon) \quad \text{if } i, j \epsilon E_k \tag{1a}$$

$$= \epsilon q_{ij} h_{ij}(t/\epsilon) \quad \text{if } i \epsilon E_k,\ j \epsilon E_k \tag{1b}$$

with $\sum_{j \epsilon E_k} p_{ij} = 1$ and where p_{ij} and q_{ij} are of order 1 and where the set of classes $\{E_k\}_{k=1}^{m}$ is disjoint and exhaustive. If the Markov chains defined by the p_{ij}'s within a single class E_k represent an ergodic Markov process with stationary state probability distribution $\{\pi_i^{(k)}\}$ for each $k (1 \leq k \leq m)$, then:

$$\lim_{\epsilon \to 0} \text{Prob}\{\text{sojourn time from class } E_k \text{ to class } E_r \leq t\} = \gamma_{kr} \cdot (1 - e^{-\lambda_k t}) \tag{2}$$

where:

$$\gamma_{kr} = \left[\sum_{i \epsilon E_k} \pi_i^{(k)} \sum_{j \epsilon E_r} q_{ij}\right] \cdot \left[\sum_{i \epsilon E_k} \pi_i^{(k)} \sum_{j \epsilon E_k} q_{ij}\right]^{-1} \tag{3}$$

$$\lambda_k = \left[\sum_{i \epsilon E_k} \pi_i^{(k)} \sum_{j \epsilon E_k} q_{ij}\right] \cdot \left[\sum_{i \epsilon E_k} \pi_i^{(k)} \sum_{j \epsilon E_k} p_{ij} \bar{\tau}_i\right] \tag{4}$$

$$\bar{\tau}_i = \sum_{j \epsilon E_k} p_{ij} \bar{\tau}_{ij} \tag{5}$$

and where $\bar{\tau}_{ij}$ is the mean holding time for the holding time

density $h_{ij}(t)$.

The proof of this theorem appears in [1] and some extensions and related results appear in [2].

Some remarks on the theorem are in order:

1. Models of fault-tolerant systems have structures similar to the conditions of the theorem in that the p_{ij} (unperturbed within-class embedded transition probabilities) are of order 1 and the embedded transition probabilities out of each class are ϵ-dependent and usually linear in ϵ where ϵ is related directly to the component failure rates. (However, see Remarks 3 and 4.)
2. The usefulness of the theorem stems from the fact that it provides an approximate description of the slow class-to-class transition dynamics over a time duration on the order of $1/\epsilon$ in terms of a finite state Markov process with only as many states as there are classes. These three properties (durations of order $1/\epsilon$, small number of states and standard Markovian behavior) are all desirable for fault-tolerant system evaluation calculations. Once the approximate interclass behavior is approximated in this way, the individual state probabilities can be approximated as:

$$\text{Prob}\{\text{occupy state } i \text{ at time } t\} = \pi_i^{(k)} \cdot \text{Prob}\{\text{occupy class } k \text{ at time } t\} \quad (6)$$

where the approximate model provides the probability on

the right-hand side.

3. Unfortunately, fault-tolerant control system models tend not to have ergodic classes E_k. In particular, systems which do not include mechanisms for on-line recovery of components declared previously to have failed yield evaluation models that include trapping states and transient states in most of the classes when ϵ is zero. For example, consider a system whose RM logic calls for permanent shutdown of a component upon declaration of its failure and which is subject to false alarms. One of the states in a model for such a system is characterized by all of the components working save one which has been shutdown by a false alarm. Assuming zero probability for component failures (i.e. $\epsilon=0$) and neglecting further false alarms, this state becomes a trapping state in the same class as the "all working" state. Therefore, the "all working" state is a transient state and the class is not ergodic for $\epsilon=0$.

4. Also unfortunately, the holding time density functions appearing in models of fault-tolerant systems tend not to have the dependence on ϵ exhibited in Eqn. (1). Consider the meaning of $h_{ij}(t/\epsilon)$ for very small ϵ: If $h_{ij}(t)$ is a typical unimodular density over $[0,\infty]$ (such as exponential, Erlang, gamma) with mean and maximum location both of order 1 in t, then $h_{ij}(t/\epsilon)$ approaches

an impulse function in t as $\epsilon \to 0$. In fault-tolerant system models, ϵ represents the component failure rate while $h_{ij}(t)$ is typically determined by the distribution of the time to decision for the appropriate RM test (particularly when i and j are both elements of the same class). Thus, $h_{ij}(t)$ is typically <u>not</u> dependent on the failure rate although it <u>does</u> typically have its mean and its maximum location at small values of t relative to the length of a mission.

Our research to the present has been directed toward applying the results of the Theorem stated above to two typical fault-tolerant control system models. In light of Remarks 3 and 4, much of our recent work has been directed toward modifications of the results of the Theorem and investigation of the effects of violating some of the conditions stated in the Theorem. The next Section briefly describes our progress in these areas.

II. Progress Summary

Our work began with a careful examination of [1] and [2] with regard to the import of the ergodic assumption discussed in Remark 3 above. This examination revealed that the proof of the Theorem above depended explicitly on the existence for each class E_k of the inverse operator $[I-P_k+\pi_k]^{-1}$ where:

I = identity operator

P_k = transition probability operator for the embedded Markov process describing transitions within class E_k after ϵ is set to zero (hence eliminating out-of-class transitions)

π_k = steady state transition operator associated with P_k, if it exists

$= \lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} P_k^i$ otherwise

As is stated in [2], if E_k is an ergodic class when $\epsilon = 0$ then $[I - P_k + \pi_k]^{-1}$ is guaranteed to exist. Hence, the ergodicity of E_k is a sufficient condition for the existence of $[I - P_k + \pi_k]^{-1}$ which in turn is a sufficient condition for the Theorem. However, ergodicity is <u>not</u> necessary for the existence of the inverse operator. As a particular example, consider a class consisting of all transient states except for a single trapping state where all of the transitions exiting the transient states enter the trapping state. Then P_k contains a row of ones in the position of the trapping state and is otherwise filled with zeroes. Then π_k has the same form. Therefore, $[I - P_k + \pi_k]^{-1} = [I]^{-1} = I$, hence the inverse operator exists. We have therefore proven the following:

<u>Proposition</u>: The results of the Theorem above are true if the Markov chain defined by the p_{ij}'s for classes $\{E_k\}$ has either of the following properties: 1) it is ergodic

with stationary state probability distribution $\{\pi_i^{(k)}\}$ (independent of the initial condition), or 2) the inverse operator $[I - P_k + \pi_k]^{-1}$ exists and a valid steady state probability distribution $\{\pi_i^{(k)}\}$ can be found such that π_k operating upon it reproduces it (and it may be dependent on the initial condition, which must then be known).

The fundamental importance of this proposition to fault-tolerant system evaluation is clear from Remark 3. Furthermore, it is relatively straightforward to numerically calculate π_k from P_k and to compute $\{\pi_i^{(k)}\}$ from π_k and the given initial condition. It is then possible to numerically evaluate the eigenvalues (or singular values) of $I - P_k + \pi_k$, which leads finally to an indication that the approximate results of the Theorem hold (and also produces the required steady state distribution $\{\pi_i^{(k)}\}$ for each k) or to an indication that the results of the Theorem do not hold.

We then proceeded to construct some typical models of fault-tolerant systems in order to test the validity of the results and to examine the conditions under which the approximation fails. Two models of fault tolerant system behaviour have been developed by Wereley. Both are based on the single-component dual-redundant (SCDR) system. This is the simplest fault tolerant configuration that may be modelled. It consists of a primary component and a backup

component with an independent failure detection test monitoring each. The RM logic is simply to use the primary component until its test indicates that it has failed at which time a switch is made to the backup unless it is already indicated to be failed.

The first model is assumed to have a sequential detection test for each component with decision time mass functions of the hypergeometric type. No recovery from false alarms is permitted. This particular model has seven states (it should be noted that the 10-JAN-85 report stated incorrectly that this was a four state model) which decompose into three distinct classes as the probability of component failure in a single time step tends to zero. Each of the three classes is non-ergodic due to the existence of a trapping state in each. This model is simple enough that analytical transform techniques, as well as numerical computations, may be used to analyze its behaviour.

The second model is also assumed to have a sequential fault detection test for each component with hypergeometric decision time mass functions. However, this model includes a false alarm recovery (FAR) test which is triggered by a detection indication. This FAR test is simply the same sequential test as for detection operating on the indicated component (that is, the component that was indicated as failed by the fault detection logic). The model has nine states

which again decompose into three distinct classes as the probability of failure tends to zero. Each of the classes is now ergodic due to the presence of the FAR test. An attempt is underway to analyze this model using analytical transform techniques using the MACSYMA symbolic manipulation software package. However, the large number of states may make symbolic manipulation impractical. In that case, numerical computations will be used to determine the behaviour of this model.

A FORTRAN program has been developed to numerically describe the behaviour of the two models. Work is currently progressing on both the transform analysis and the application of the approximation techniques to these two relatively simple models.

Meanwhile, work has also been started on a more complex, more realistic fault-tolerant system model similar to the one described in [3]. Kwong has constructed a model for a fault tolerant system with 3 redundant components, which employs the Vector Shiryayev Sequential Test (VSST) (see [3]) to identify and isolate failed components. The model is a 9-state continuous parameter semi-Markov process. In the system, when a component is isolated by the VSST, a self-test is initiated and the component will be brought back into operation when there are two consecutive no-failure indications from the self-test. The semi-Markov model can be decomposed into 3

disjoint classes when the failure rate, ϵ, of each component is equal to zero. The classes are ergodic. Numerical results for ϵ = 2.5 x 10e-6 failures per second, show that the normalized probabilities of occupying each state within each class converge to the steady state probabilities of the non-perturbed system for each class. Also, the steady state probability distribution of the non-perturbed system can be evaluated analytically. Therefore, the state probabilities of the perturbed system can be approximated analytically if the total probability within each class is known as a function of time.

The results of Korolyuk and Turbin's theorem can be applied to obtain the approximate total probabilities within each class when time is scaled by a time-scaling factor. Results of the analytical calculation and of a complete numerical calculation are compared in Table 1 in terms of the total probability of occupying each class. As one would expect, the results are in relatively close agreement, never differing by more than about 10%. By examining other values of ϵ, it was empirically found that $\epsilon > 10^{-5}$ led to discrepancies in the results. It is of interest to note that this is just two orders of magnitude smaller than the smallest decision time rate assumed for the tests (see Table 1).

Table 1. Exact Results vs. Approximate Results for Class Probabilities: 9-State Model

Model parameters:

Component failure rate: 2.5×10^{-6} sec $^{-1}$

False alarm decision rate: 10^{-3} sec $^{-1}$

Detection decision rate: .05 sec^{-1}

Recovery test false alarm rate: .05 sec $^{-1}$

Recovery test recovery rate: .1 sec^{-1}

Recovery test validation rate: .1 sec^{-1}

Recovery test miss rate: .05 sec $^{-1}$

Probability of Occupying Class

(Exact: top line; Approximate: bottom)

Time(sec.)	Class 1	Class 2	Class 3
40	.9997001	.0002999	3×10^{-8}
	.9997000	.0002999	3×10^{-8}
280	.9979038	.0020949	.0000013
	.9979022	.0020963	.0000015
600	.9955171	.0044769	.0000061
	.9955101	.0044832	.0000067
1200	.9910621	.0089137	.0000241
	.9910404	.0089328	.0000269
1600	.9881047	.0118525	.0000428
	.9880717	.0118806	.0000477

We have also constructed a four-state model for the purpose of examining the impact of nonergodicity on the results. The basic four-state model involves "fast" transitions between states 1 and 2 with "slow" transitions occurring between these states and the remaining two states. All transitions are semi-Markov in nature with second-order hyperexponential holding time pdf's. Several variations of this model are currently under study, some with ergodic classes and some with nonergodic classes. The results are now being generated and should be available late in the Fall.

We have also partially completed an analytical effort to circumvent the difficulty discussed in Remark 4 above. This involves the introduction of a second small parameter into the description of the process as a time-scaling parameter. Recall from Eqn. (1) that in order to apply the results of Korolyuk's theorem or our proposition, the transition kernel elements of the perturbed process had to take the form:

$$p^{\epsilon}_{ij} h_{ij}(t/\epsilon)$$

where p^{ϵ}_{ij} is proportional to ϵ for interclass transitions but is asymptotically (as $\epsilon \to 0$) independent of ϵ for intraclass transitions. Consider now replacing this form by:

$$p^{\epsilon}_{ij} h_{ij}(t/\delta)$$

where p^{ϵ}_{ij} is the same as before. The asymptotic results of the theorem remain true if δ is such that $\delta = C\epsilon$ with $\epsilon \ll C \ll \frac{1}{\epsilon}$). This can be seen from Korolyuk's proof [1]. Note

that δ is now a time-scaling parameter which is small. Now consider finding asymptotic results as ϵ and δ approach zero separately. In effect, this is what we have done with our modification. We do not have a rigorous proof as yet that the results are still asymptotically true (except for the case cited above), but the empirical results so far have all been supportive. We will expand on this topic in the coming months.

III. Papers and Presentations Derived from This Work

A presentation was made at the following Workshop:

AFOSR Workshop on Reliability
Skyland Lodge
Shenandoah National Park, Virginia
May 28-31, 1985

The abstract and viewgraphs from this presentation appear in Appendix I.

A brief reference to this work is contained in a paper presented at a Conference in July:

B.K. Walker & D.K. Gerber, "Evaluation of Fault-Tolerant System Performance by Approximate Techniques", Proc. of 7th IFAC Symp. on Identification & System Parameter Estimation, York, UK, July 1985.

A copy of this paper appears in Appendix II.

IV. Projections for Second Year of Work

Our efforts will continue on the models discussed in this report. Of particular interest will be the results for models with nonergodic classes and the efforts to employ two small parameters in the description of the model. Furthermore, we expect to be able to analyze some of the smaller models analytically using a symbolic manipulation program called MACSYMA. This will allow us to derive closed form transform solutions for the smaller models which can be examined easily for their asymptotic properties as the failure rate parameter becomes small.

We also plan to construct a more realistic model similar to the nine-state model cited above. This model will use actual holding time pdf data derived from simulations of sequential fault diagnosis tests such as the VSST. This will provide the information necessary to apply the approximate results that we have derived (or modified) to a realistic fault-tolerant system model.

In light of the many questions that have arisen as part of our inquiries (particularly regarding the rigorous justification for some of our analytical results), we anticipate the need for further work and hence we plan to submit a proposal to continue this work beyond next summer.

V. Financial & Manpower Status

The manpower remains as it was proposed. Prof. Bruce K. Walker devotes approximately 20% of his time to the project, primarily in a supervisory capacity. Two graduate students, Siu-Kwong Chu and Norman M. Wereley, work as full-time graduate research assistants on the project. Margaret McCabe devotes approximately 10% of her time to the project for clerical support. No changes are anticipated.

With regard to the financial status, a substantial cost underrun occurred in the first year of the project primarily due to the timing of the project. A proposal will be submitted to carry over the leftover funds into the second year. Any significant changes proposed for the second year of funding will accompany that proposal.

References

[1] V.S. Korolyuk, L.I. Polischuk, and A.A. Tomusyak, "A Limit Theorem for Semi-Markov Processes," Kybernetika, 5:4:144-145, July-Aug. 1969.

[2] V.S. Korolyuk and A.F. Turbin, "Asymptotic Enlarging of Semi-Markov Processes with an Arbitrary State Space," in A. Dold & B. Eckmann (eds.), Lecture Notes in Mathematics 550: Proceedings of the 3rd Japan - USSR Symposium on Probability Theory, Springer-Verlog, 1972.

[3] B.K. Walker, "A Semi-Markov Approach to Quantifying Fault-Tolerant System Performance," Sc.D. thesis, Dept. of Aeronautics & Astronautics, M.I.T., July 1980.

APPENDIX I

DECOMPOSITION OF GENERALIZED MARKOVIAN MODELS OF FAULT-TOLERANT SYSTEMS - MOTIVATION, PROGRESS AND PROBLEMS

Bruce K. Walker
Assistant Professor
Department of Aeronautics and Astronautics
Massachusetts Institute of Technology

Siu-Kwong Chu
Norman Werely
Graduate Research Assistants
Department of Aeronautics and Astronautics
Massachusetts Institute of Technology

These three presentations will summarize our work to date on decomposition methods applied to Markovian models of fault-tolerant system behavior. Such models are very useful as design tools for the evaluation of the reliability and performance of various fault-tolerant system designs.

First, we shall present the concept of modelling fault-tolerant system behavior by Markovian models. We shall discuss the construction of Markov models for systems which use on-line fault diagnostic tests of the "single sample" variety. This will illustrate the generality of this modelling method and the useful performance results which can be generated by such models. It will also illustrate some of the practical problems that arise when complex systems are considered. We shall then discuss the extension of these modelling techniques to systems which use "sequential" on-line diagnostic tests. This requires the generalization of the modelling technique to include semi-Markovian models. It leads to further applicability of the modelling method and also to further practical problems for complex systems.

Next, we shall present as an illustrative example the relatively simple case of a single dual-redundant component with on-line diagnostics which are used to implement a primary/backup operating strategy. The Markov model for this system will be presented and reliability results will demonstrate that as the component mean time to failure (MTTF) becomes large relative to the time increment between fault diagnosis testing a decomposition of the model becomes apparent. A semi-Markov model will then be developed for this system and similar results will be presented. We shall then discuss our efforts to generate analytical results based upon the decomposition of this model when the holding time densities of the semi-Markov model are of a particularly simple yet relevant form (namely hypergeometric of order 2).

Finally, we shall review our progress since last fall on our efforts to apply the analytical results of Korolyuk and Turbin to our models. We shall discuss the points at which models of fault-tolerant systems violate the sufficient conditions for application of those results and how the conditions can be relaxed or modified. We shall also present some numerical results that indicate the need for extension of some of the approximations. We shall discuss our approach to achieving such an extension.

DECOMPOSITION OF GENERALIZED MARKOVIAN MODELS OF FAULT-TOLERANT SYSTEMS:

- MOTIVATION,
- PROGRESS, AND
- PROBLEMS

BRUCE K. WALKER, ASSISTANT PROF.
SIU-KWONG CHU, GRADUATE RESEARCH ASSISTANT
NORMAN M. WERELEY, GRADUATE RESEARCH ASSISTANT

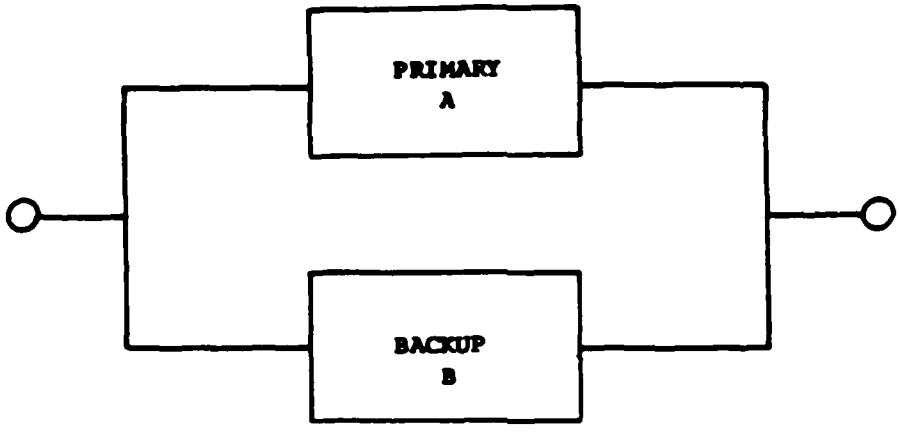
DEPARTMENT OF AERONAUTICS & ASTRONAUTICS
MASSACHUSETTS INSTITUTE OF TECHNOLOGY
CAMBRIDGE, MA 02139

SPONSORED BY: AFOSR
GRANT: AFOSR-84-0160

AFOSR RELIABILITY WORKSHOP
SKYLAND LODGE
LURAY, VA
MAY 29-31, 1985

A "SIMPLE" EXAMPLE

A SINGLE DUAL-REDUNDANT INSTRUMENT WITH THE STRUCTURE BELOW:

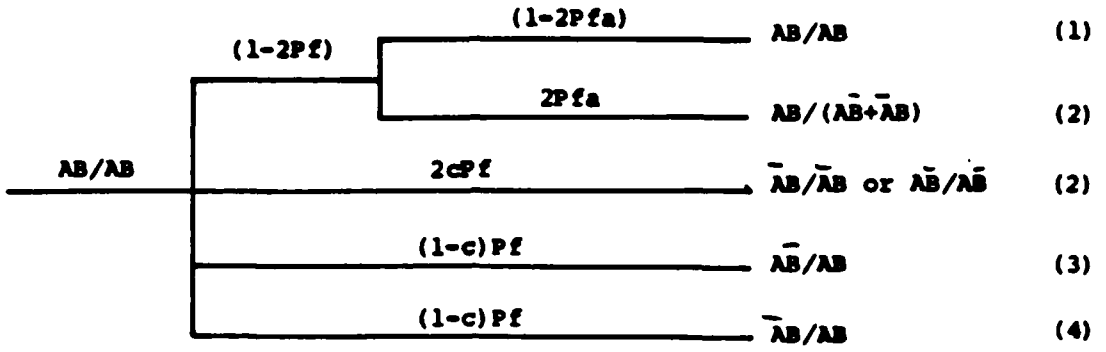


HAS THE FOLLOWING REDUNDANCY MANAGEMENT (RM) POLICY:

- EACH INSTRUMENT HAS AN INDEPENDENT FAILURE DETECTION TEST
- THE PRIMARY INSTRUMENT IS USED UNTIL A FAILURE OF THE PRIMARY IS INDICATED, IN WHICH CASE THE PRIMARY IS TURNED OFF AND THE BACKUP INSTRUMENT IS USED
- THE FAILURE DETECTION TESTS ARE TURNED OFF AFTER THE FIRST INDICATED FAILURE
- THE SYSTEM WORKS IF A WORKING INSTRUMENT IS BEING USED

A HOMOGENEOUS MARKOV MODEL WILL BE DEVELOPED FOR THE ABOVE RM POLICY. NOTE THAT A FAILURE DETECTION DECISION IS AVAILABLE AT EVERY TIME STEP.

EVENT TREE FOR TRANSITIONS FROM STATE 1



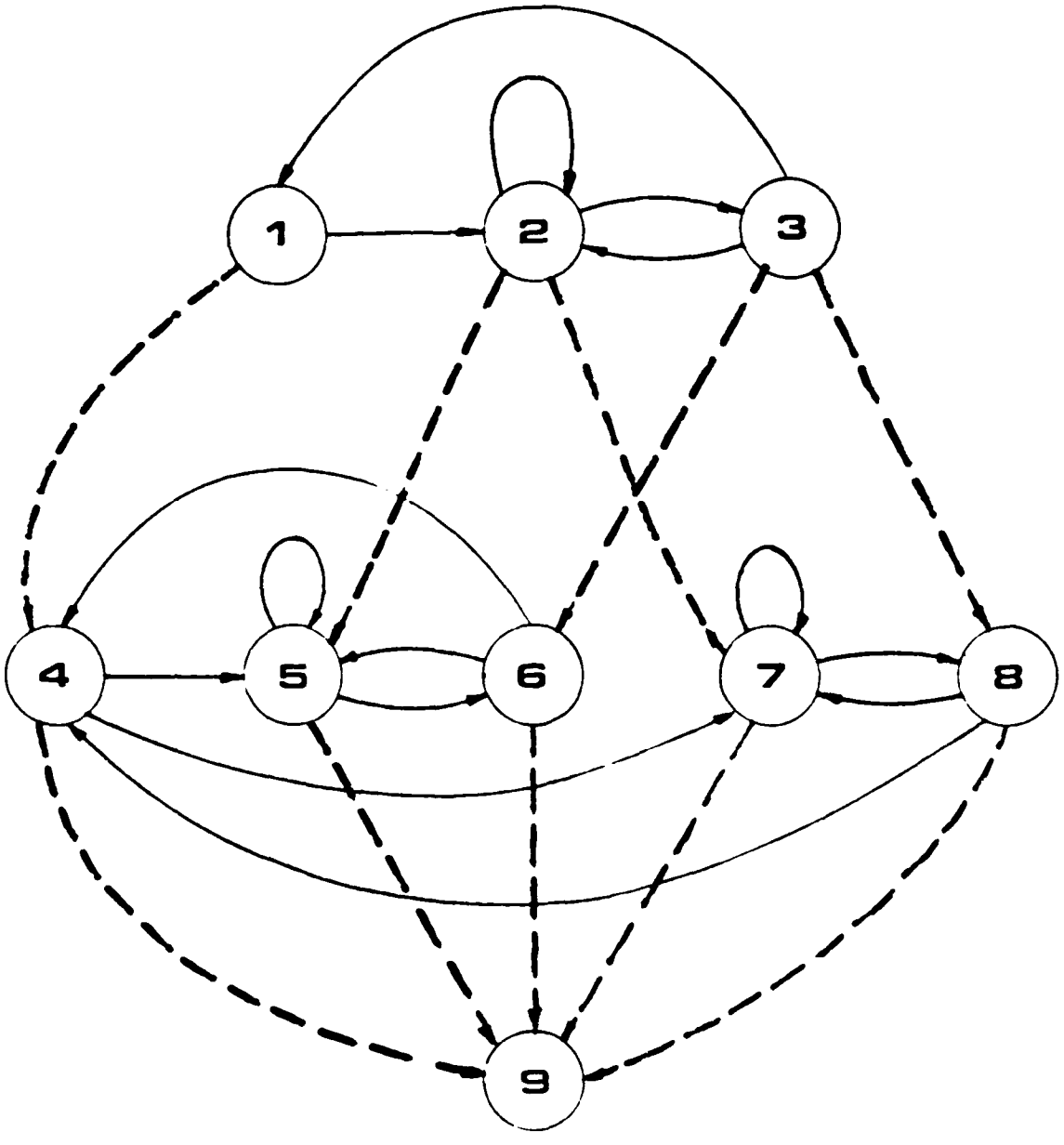
STATE DEFINITIONS

1. BOTH INSTRUMENTS WORKING
2. ONE INSTRUMENT WORKING, THE OTHER TURNED OFF DUE TO AN INDICATED FAILURE
3. BACKUP COMPONENT FAILED UNCOVERED
4. SYSTEM LOSS

BOTH THE PROBABILITY OF FAILURE OVER ONE TIME STEP Pf AND THE PROBABILITY OF FALSE ALARM OVER ONE TIME STEP Pfa ARE SMALL NUMBERS - TYPICALLY 10^{-6}.

SINGLE-STEP STATE TRANSITION PROBABILITY MATRIX

$$P = \begin{bmatrix} 1-2(Pf+Pfa) & 0 & 0 & 0 \\ 2(Pfa+cPf) & 1-Pf & c(1-Pf-Pfa) & 0 \\ (1-c)Pf & 0 & (1-c)(1-Pf-Pfa) & 0 \\ (1-c)Pf & Pf & Pf+Pfa & 1 \end{bmatrix}$$



Transition Diagram

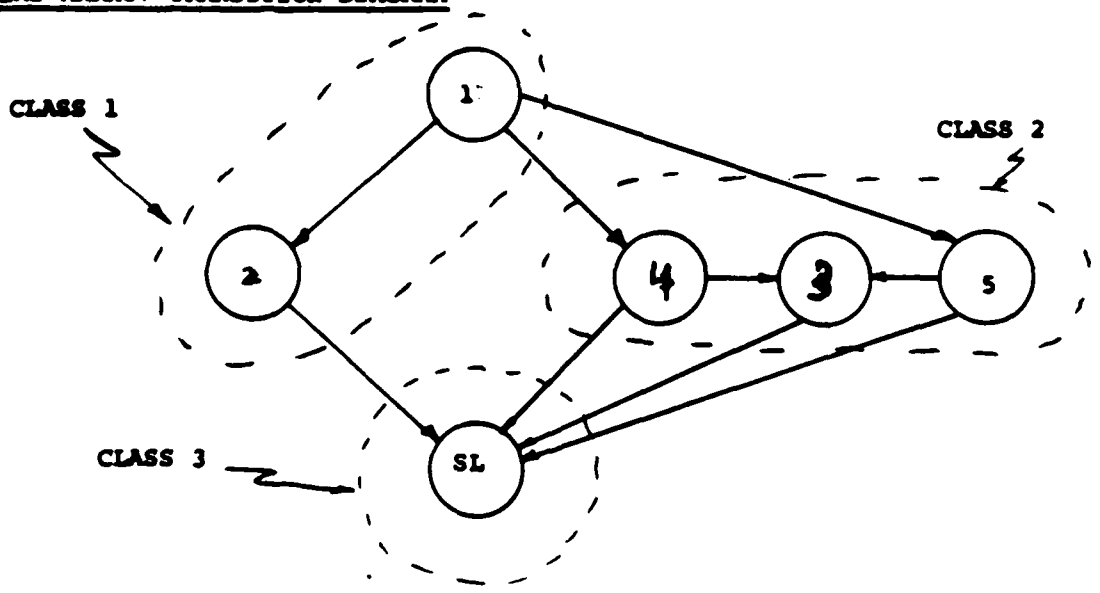
NEW RM POLICY

- EACH INSTRUMENT HAS AN INDEPENDENT SEQUENTIAL PROBABILITY RATIO TEST (SPRT) TO DETECT FAILURES
- BOTH TESTS ARE RESET ON ANY NOMINAL INDICATION
- DECLARE FAILURE OF AN INSTRUMENT WHEN ITS SPRT INDICATES A FAILURE
- THE PRIMARY INSTRUMENT IS USED UNTIL A FAILURE OF THE PRIMARY IS INDICATED, IN WHICH CASE THE PRIMARY IS TURNED OFF AND THE BACKUP IS USED
- THE FAILURE DETECTION TEST IS TURNED OFF AFTER THE FIRST INDICATED FAILURE
- THE SYSTEM WORKS IF A WORKING INSTRUMENT IS BEING USED BUT IS ROBUST ENOUGH TO SUSTAIN A FAILURE FOR A "WHILE"

STATE DEFINITIONS FOR THE SEMI-MARKOV MODEL

1. BOTH INSTRUMENTS WORKING
2. ONE INSTRUMENT WORKING, THE OTHER TURNED OFF DUE TO A FALSE ALARM
3. ONE INSTRUMENT WORKING, THE OTHER TURNED OFF DUE TO A COVERED FAILURE
4. PRIMARY INSTRUMENT FAILURE - NO INDICATION YET
5. BACKUP INSTRUMENT FAILURE - NO INDICATION YET.
6. SYSTEM LOSS

SEMI-MARKOV TRANSITION DIAGRAM



COMPUTATIONAL TIME FOR EACH $\bar{\Phi}(n)$ OF A SEMI-MARKOV PROCESS

interval transition probabilities matrix is generated by the following equation,

$$\bar{\Phi}(n) = \bar{W}(n) + \sum_{m=1}^{n} C(m)\,\bar{\Phi}(n-m) \qquad n = 0, 1, 2 \cdots$$

with initial condition $\bar{\Phi}(0) = I$

$$\bar{\Phi}(1) = \bar{W}(1) + C(1)\,\bar{\Phi}(0)$$

$$\bar{\Phi}(2) = \bar{W}(2) + C(1)\,\bar{\Phi}(1) + C(2)\,\bar{\Phi}(0)$$

$$\bar{\Phi}(n) = \bar{W}(n) + \underbrace{C(1)\,\bar{\Phi}(n-1) + \cdots + C(n)\,\bar{\Phi}(0)}_{n \text{ terms}}$$

let computational time required for each $C(m)\,\bar{\Phi}(n-m) = 1$ unit, therefore computational time required for calculating $\bar{\Phi}(n)$ is

$$= 1 + 2 + 3 + \cdots + n$$
$$= \frac{(n+1)}{2} n$$
$$\approx n^2 \text{ units}$$

number of floating point multiplications required for calculating $\bar{\Phi}(36000)$ of a 9 states semi-Markov process is

$$= (36000)^2 \times (9)^3$$
$$= 9.44 \times 10^{11}$$

normalized probabilities distribution for various ϵ

tate	$\epsilon=0$	$\epsilon=1.0E-6$	$\epsilon=2.5E-5$	$\epsilon=2.5E-5$	$\epsilon=1.0E-4$	$\epsilon=1.0E-3$	$\epsilon=5.0E-3$	$\epsilon=2.5E-2$
1	0.[illegible]738	0.[illegible]765	[illegible]	0.9765	0.[illegible]713	0.9755	0.8715	0.3982
2	0.0725	0.0711	[illegible]	0.0711	0.[illegible]712	0.0715	0.0732	0.4571
3	0.[illegible]97	0.[illegible]	[illegible]	0.0524	0.[illegible]	0.0530	0.0553	0.1447
total probability in 1st. class		0.[illegible]	[illegible]	0.9737	0.[illegible]	0.9442	0.4841E-2	0.5939E-1
4	0.1175	0.[illegible]7	[illegible]	0.2063	0.[illegible]	0.1919	0.1485	0.1103
5	0.4575	0.[illegible]	[illegible]	0.6057	0.[illegible]	0.[illegible]	0.6590	0.6941
6	0.1783	0.1[illegible]	[illegible]	0.1493	0.1[illegible]	0.1536	0.1673	0.1214
7	0.[illegible]	0.[illegible]	[illegible]	0.0193	0.[illegible]	0.0185	0.0140	0.0080
8	0.[illegible]	0.[illegible]	[illegible]	0.0159	0.[illegible]	0.[illegible]	0.0111	0.0063
total probability in 2nd. class		0.[illegible]	[illegible]	0.2c10E-1	0.[illegible]	0.4553	0.c709E-1	0.2439E-6
9	1.	1.	1.	1.0	1.[illegible]	1.0	1.[illegible]	1.0
total probability in 3rd. class		0.[illegible]	[illegible]	0.2[illegible]3E-3	0.1[illegible]2E-1	0.2005	0.9081	0.9999

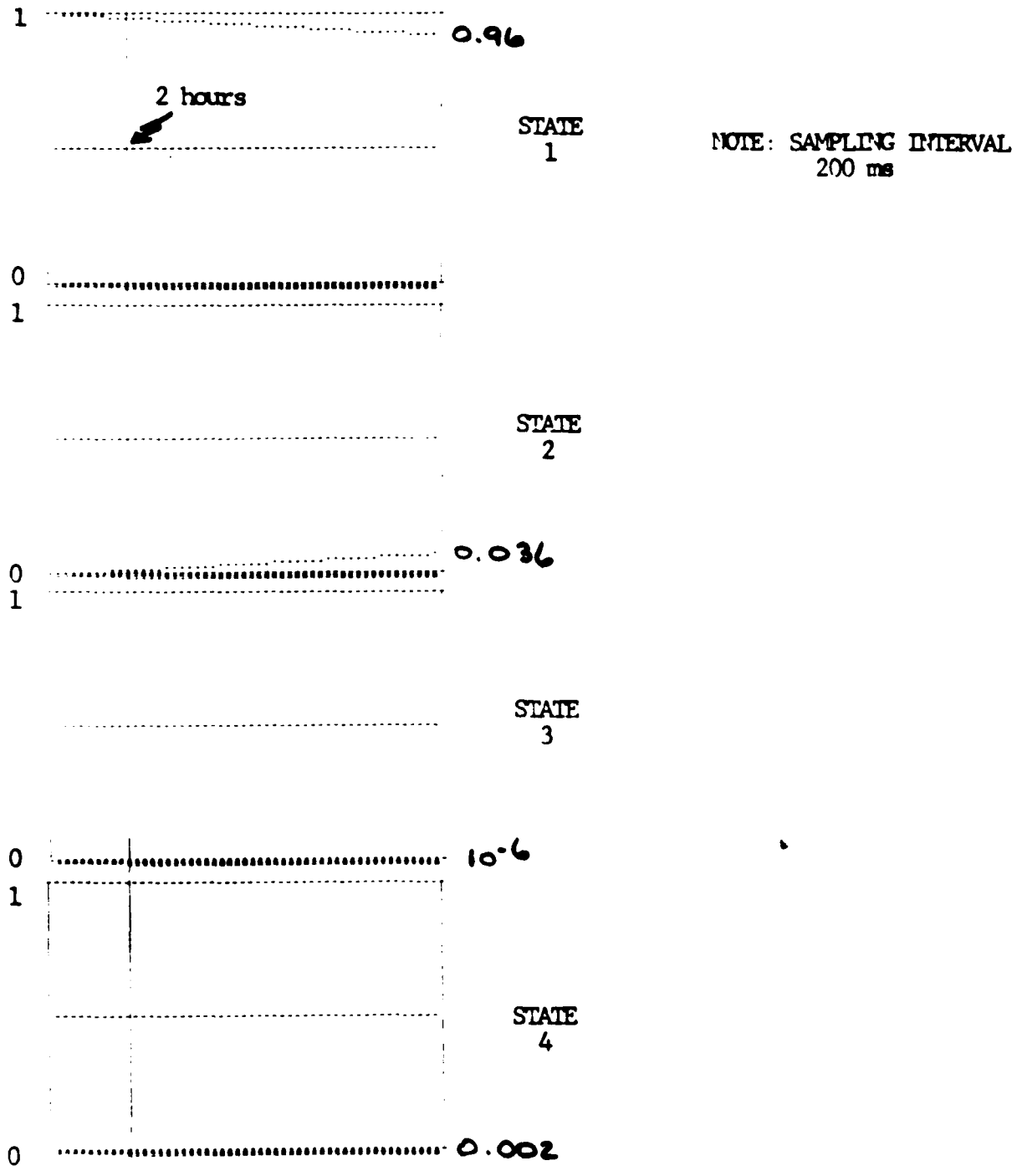
Δt= 4 sec.
time step= 50

DUAL-REDUNDANT SYSTEM PERFORMANCE USING MARKOV MODELS

THE STATE OCCUPANCY PROBABILITIES ARE PLOTTED BELOW UNDER THE FOLLOWING CONDITIONS:

MTBF = 500 hours
MISSION TIME = 2 hours
COVERAGE PROBABILITY = 0.8

MTTPA = 500 hours
TIME AXIS = 10 hours



ep	lam0	lam1	lamw0	lamw1	lamf0	lamf1
0. e+00	0.50e-02	0.50e-01	0.50e-01	0.10e+00	0.10e+00	0.50e-01

no. of time step = 250
time step/sec = 4.00
final time = 1000.00

normalised prob. dist in each class

time step	state 1	2	3	4	5	6	7	8
10	0.9835e+00	0.1246e-01	0.4070e-02	0.4169e+00	0.4656e+00	0.6374e-01	0.3610e-01	0.1765e-01
20	0.9530e+00	0.3034e-01	0.1663e-01	0.1642e+00	0.6308e+00	0.1486e+00	0.2738e-01	0.2405e-01
30	0.9264e+00	0.4490e-01	0.2869e-01	0.1319e+00	0.6633e+00	0.1587e+00	0.1740e-01	0.1577e-01
40	0.9075e+00	0.5512e-01	0.3768e-01	0.1266e+00	0.6759e+00	0.1538e+00	0.1288e-01	0.1081e-01
50	0.8944e+00	0.6181e-01	0.4374e-01	0.1220e+00	0.6822e+00	0.1562e+00	0.1095e-01	0.8661e-02
60	0.8864e+00	0.6601e-01	0.4762e-01	0.1198e+00	0.6851e+00	0.1573e+00	0.1008e-01	0.7716e-02
70	0.8814e+00	0.6860e-01	0.5003e-01	0.1187e+00	0.6865e+00	0.1578e+00	0.9687e-02	0.7289e-02
80	0.8783e+00	0.7017e-01	0.5150e-01	0.1183e+00	0.6871e+00	0.1581e+00	0.9508e-02	0.7091e-02
90	0.8765e+00	0.7111e-01	0.5239e-01	0.1180e+00	0.6874e+00	0.1582e+00	0.9426e-02	0.7006e-02
100	0.8754e+00	0.7167e-01	0.5292e-01	0.1180e+00	0.6875e+00	0.1582e+00	0.9389e-02	0.6969e-02
110	0.8748e+00	0.7200e-01	0.5324e-01	0.1179e+00	0.6875e+00	0.1582e+00	0.9373e-02	0.6954e-02
120	0.8744e+00	0.7220e-01	0.5342e-01	0.1179e+00	0.6876e+00	0.1583e+00	0.9365e-02	0.6948e-02
130	0.8741e+00	0.7232e-01	0.5353e-01	0.1179e+00	0.6876e+00	0.1583e+00	0.9362e-02	0.6945e-02
140	0.8740e+00	0.7239e-01	0.5360e-01	0.1179e+00	0.6876e+00	0.1583e+00	0.9360e-02	0.6944e-02
150	0.8739e+00	0.7243e-01	0.5364e-01	0.1179e+00	0.6876e+00	0.1583e+00	0.9359e-02	0.6943e-02
160	0.8739e+00	0.7245e-01	0.5366e-01	0.1179e+00	0.6876e+00	0.1583e+00	0.9359e-02	0.6943e-02
170	0.8739e+00	0.7246e-01	0.5367e-01	0.1179e+00	0.6876e+00	0.1583e+00	0.9359e-02	0.6942e-02
180	0.8738e+00	0.7247e-01	0.5368e-01	0.1179e+00	0.6876e+00	0.1583e+00	0.9359e-02	0.6932e-02
190	0.8738e+00	0.7248e-01	0.5369e-01	0.1179e+00	0.6876e+00	0.1583e+00	0.9359e-02	0.6932e-02
200	0.8738e+00	0.7248e-01	0.5369e-01	0.1179e+00	0.6876e+00	0.1583e+00	0.9359e-02	0.6932e-02
210	0.8738e+00	0.7248e-01	0.5369e-01	0.1179e+00	0.6876e+00	0.1583e+00	0.9359e-02	0.6932e-02
220	0.8738e+00	0.7248e-01	0.5369e-01	0.1179e+00	0.6876e+00	0.1583e+00	0.9359e-02	0.6932e-02
230	0.8738e+00	0.7248e-01	0.5369e-01	0.1179e+00	0.6876e+00	0.1583e+00	0.9359e-02	0.6932e-02
240	0.8738e+00	0.7248e-01	0.5369e-01	0.1179e+00	0.6876e+00	0.1583e+00	0.9359e-02	0.6932e-02
250	0.8738e+00	0.7248e-01	0.5369e-01	0.1179e+00	0.6876e+00	0.1583e+00	0.9359e-02	0.6932e-02

normalized prob. dist. in state 9 always eq. to 1

NORMALIZED STATE PROBABILITIES TRAJECTORY FOR $\epsilon = 0$

state	$\epsilon = 2.5 \times 10^{-6}$ unnormalized probabilities distribution	$\epsilon = 2.5 \times 10^{-6}$ normalized probabilities distribution	$\epsilon = 0$	normalized probabilities distribution (analytical result)
1	0.8535	0.8738	0.8738	0.8856
2	0.0708	0.0725	0.0725	0.0658
3	0.0524	0.0537	0.0537	0.0487
total probability in 1st. class	0.9767	1.0	1.0	1.0
4	0.0030	0.1279	0.1179	0.1250
5	0.0157	0.6786	0.6875	0.6820
6	0.0040	0.1750	0.1783	0.1768
7	0.0002	0.0106	0.0094	0.0093
8	0.0002	0.0080	0.0069	0.0069
total probability in 2nd. class	0.0231	1.0	1.0	1.0
9	0.0002	1.0	1.0	1.0

$\Delta t = 4$ sec.

time step = 800

An Approximation (Korolyuk & Turbin, 1976)

Perturbed semi-Markov chain: $\xi^{\varepsilon}(t)$ with ε a small parameter,

State space partitions into m disjoint classes $E_1, \ldots, E_m$ where kernel matrix is:

$$P_{ij}^{\varepsilon}(t) = p_{ij}^{\varepsilon} \, h_{ij}(t/\varepsilon)$$

$$p_{ij}^{\varepsilon} = \begin{cases} p_{ij} - \varepsilon q_{ij} & \text{for } i, j \in E_k \\ \varepsilon q_{ij} & i \in E_k,\ j \in E_r,\ r \neq k \end{cases}$$

For each class E_k, stationary distribution $\{\pi_i^{(k)}\}$ exists (always true if each class is ergodic),

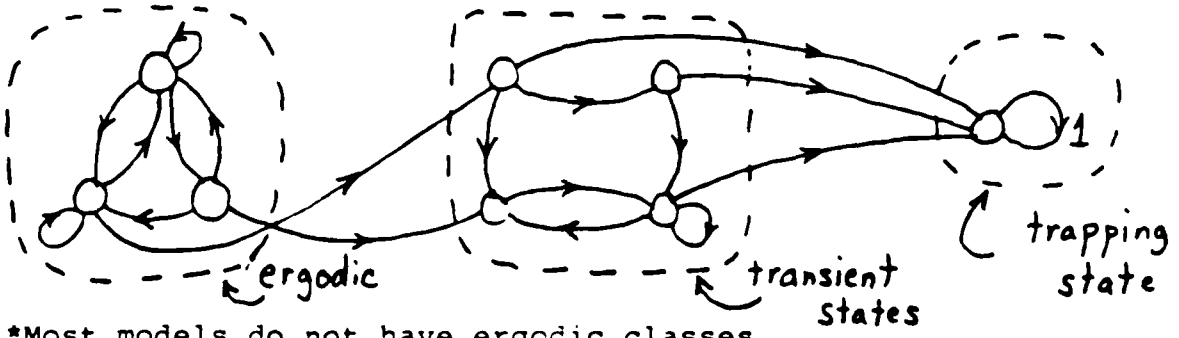
Then: As $\varepsilon \to 0$,

$$\text{Prob}\{\xi^{\varepsilon}(\tfrac{t}{\varepsilon}) = i\} \cong \pi_i^{(k)} \cdot \text{Prob}\{\gamma(t) = k\} \quad (i \in E_k)$$

where $\gamma(t)$ is a Markov process representing class-to-class transition behavior with mean time to transition dependent on mean holding times and q_{ij}'s.

Problem: Ergodicity of Classes

Typical fault-tolerant system model:



*Most models do not have ergodic classes

- Ergodicity is sufficient but not necessary.
- Also sufficient is existence of the inverse operator for each class:

$$[I - P + \pi]^{-1}$$

where: P is interval transition probability operator,
π is Cesaro limit of successive P operations, i.e.

$$\pi = \lim_{n \to \infty} \frac{1}{n} \sum_{k=1}^{n} P^k$$

(generates stationary operator if a stationary distribution exists)

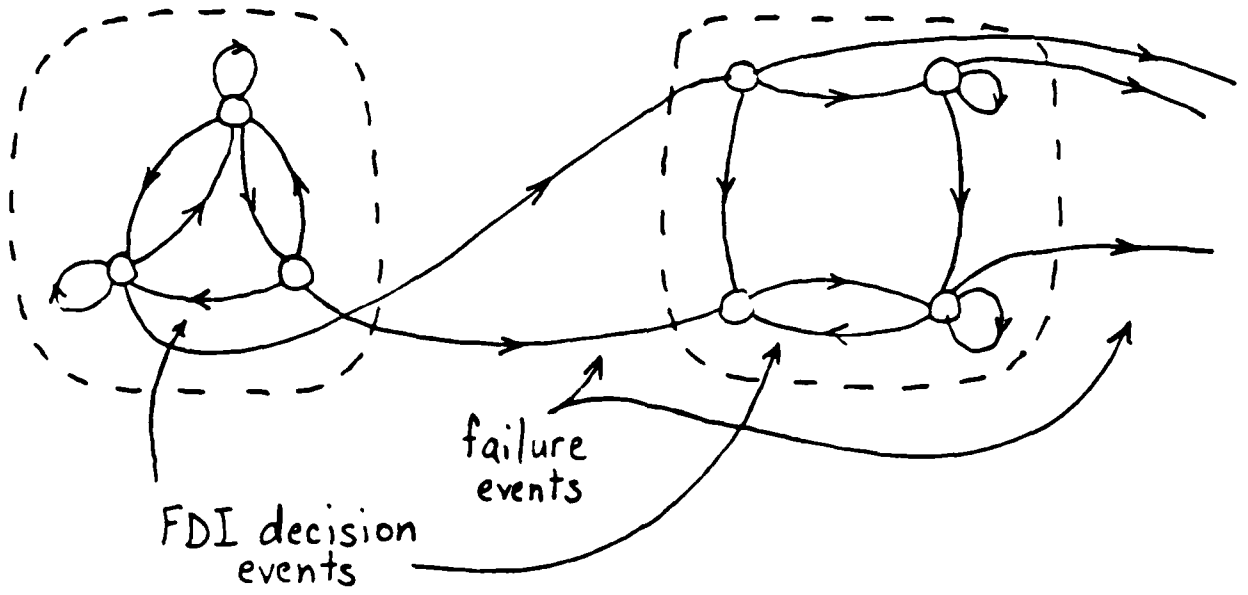
- Can check for this existence numerically.

Problem: ε - dependence

Our first case:

$$P^{\varepsilon}_{ij}(t) = p^{\varepsilon}_{ij}\, h_{ij}(t)$$

Holding time pdf not dependent on ε (which corresponds to failure rate in fault-tolerant system models).



$\tau_{kr}(s) \triangleq$ L {Sojourn time from class k to class r, $k \neq r$}

(Yields Markovian behavior of Y in original approximation.)

SEMI-MARKOV KERNEL FOR THE CLASS TO CLASS PROCESS

$\varphi_{kr}^{(u)}(s)$: Laplace transform of semi-Markov kernel for the process starts from state i in class E_k and moves to E_r

$p_{ij}^{e}(s)$: Laplace transform of semi-Markov kernel

$$p_{ij}^{e}(s) = \begin{cases} p_{ij}^{(k)} H_{ij}(s) - \varepsilon_{ij}^{(k)} H_{ij}^{e}(s) & i,j \in E_k \\ \varepsilon_{ij}^{(k)} h_{ij}(s) & i \in E_k \quad j \in E_r \end{cases}$$

assume $\varphi_{kr}(s)$ is independent of superscript,

then one can deduce

$$\varphi_{kr}(s) = \frac{\sum_{i \in E_k} \pi_i^{(k)} \sum_{j \in E_r} q_{ij}^{(k)} h_{ij}(s)}{\sum_{i \in E_k} \pi_i^{(k)} \sum_{j \in E_k} q_{ij}^{(k)} H_{ij}^{e}(s)}$$

WHAT FORM IS $\varphi_{21}(s)$ LIKE FOR THE MODEL

assume $\lambda_c, \lambda_{w_0}, \lambda_{w1}$ have the numerical values such that $\pi_1^{(1)} \gg \pi_2^{(1)}$ and $\pi_3^{(1)}$

$$\varphi_{21}(s) = \frac{\pi_1^{(1)} q_{21}^{(1)} h_{21}(s)}{\pi_1^{(1)} q_{21} H_{21}^{\dagger}(s)}$$

$$= \frac{\dfrac{3s + 6\lambda_c + 9\varepsilon}{[s + (\lambda_0 + 3\varepsilon)]^2}}{\dfrac{6(\lambda_c + 3\varepsilon)}{\lambda_0[s + (\lambda_c + 2\lambda_0)]^2}}$$

$$= \frac{3s + 6\lambda_c + 9\varepsilon}{6\lambda_c + 9\varepsilon}$$

$$\approx \frac{3s + 6\lambda_0}{6\lambda_0} \qquad \text{as } \varepsilon \to 0$$

$\varphi_{21}^{(1)}$ does not depend on ε (?)

MATCHING THE CONDITIONS STATED IN THE PAPER

- propose the semi-Markov process depending ontwo small parameters ε and δ

  ε : class to class transition parameter

  δ : time scaling parameter

  as ε and $\delta \to 0$

  * semi-Markov process, state space E can be split into disjoint classes of states $E=\sum_{k=1}^{m} E_k$
  * the sojourn of the process in a given state tends to zero

- trying to validate two small parameters method and deduce $\varphi_{kr}(s)$

CURRENT WORK

- CONTINUE "SIMPLE" MODEL
  - NONERGODIC CLASSES
  - SMALL ENOUGH FOR ANALYTICAL TRANSFORMS
  - FURTHER NUMERICAL RESULTS
- USE TWO SMALL PARAMETERS TO EXTEND ANALYSIS OF LARGER MODEL
  - HAS ERGODIC CLASSES
- FURTHER EXAMPLES
  - INVERSE OPERATOR CALCULATION (FOR EXISTENCE)

APPENDIX II

EVALUATION OF FAULT-TOLERANT SYSTEM PERFORMANCE BY APPROXIMATE TECHNIQUES

Bruce K. Walker

Dept. of Aeronautics and Astronautics, Massachusetts Institute of Technology, Cambridge, Massachusetts, USA

David K. Gerber

United States Air Force, Williams AFB, Arizona, USA

Abstract. An approximate method for calculating the statistics of the performance of a fault-tolerant system is developed. An approximate method is necessary because the statistical model of the system behavior is large-scale and the time horizon of interest encompasses many cycles of the Redundancy Management logic. In the development, a compact representation of the necessary information called the v-transform is introduced and discussed. Based upon this representation, an approximation that leads to a very efficient computational procedure is suggested and numerically analyzed. A very brief discussion of other related work is also presented.

Keywords. System failure and recovery; reliability theory; Markov processes; stochastic systems; numerical methods

1. Introduction

The use of imbedded microprocessors and other computational devices in the implementations of control system designs has given the designer of such systems the freedom to synthesize very complex control schemes. The motivation for using such sophisticated designs is the significant enhancement of the system performance which can be obtained relative to designs which use very crude control strategies. These sophisticated designs often involve the use of many sensing and actuating components in an integrated control scheme. The components are often subject to failure or damage, and it is often the case that the system performance degrades dramatically or even becomes unacceptable or unsafe when one or more of the components ceases normal operation. Examples of such systems include digital flight control systems for statically unstable aircraft (such as the X-29), the flight and engine control systems for VTOL aircraft, the attitude and shape control systems for large space vehicles, and the control systems of nuclear power plants.

The fundamental importance of certain components to the acceptable or optimal performance of the control system has led to the incorporation of redundancy and fault-tolerance into such systems. Fault-tolerance may be achieved either by replicating the hardware components which are subject to faults or by implementing a system which provides functional redundancy among its components. In either case, the automatic control system is then obliged to manage this redundancy by monitoring the components for faults and selecting the components to be used in real time. This function of the automatic system is referred to as Redundancy Management (RM). Its implementation can be as simple as a passive signal selection scheme from among replicated identical sensors, or as complex as a sophisticated configuration selection scheme based on automated logic which utilizes elements of statistical decision theory.

The presence in the system implementation of a Redundancy Management function lends a different meaning to the concept of system performance. The optimal design performance will only be achieved (or approached) if all of the components remain operational and the RM function performs flawlessly. If either of these conditions are violated, the system will in general perform less than optimally. This suggests that the "performance" of the system is not the optimal performance that is attainable when everything is working properly but rather is a random variable which reflects the occurrence of random component failures and random RM decision errors. The statistical properties of this random "performance" value is of great interest to the designer of the system. It is the calculation of these statistical performance properties with which we shall concern ourselves in this paper. The computational algorithms which result from the analysis can be thought of as design tools for the fault-tolerant control system designer.

Since component failures and RM decisions can both be characterized as random events, one of the primary steps in the development of a performance evaluation method is the construction of a stochastic model for those aspects of the behavior of the system which govern the performance. There exist two approaches to this modelling task: the combinatorial method [1] and the method of generalized Markovian models [2]. It has been shown that the former method is far more unwieldy than the latter when it is necessary to account for the time ordering of the random events which may take place during a mission [3,4]. Since the system performance may be impacted dramatically by such time-ordered events, this makes the latter method far more attractive. Henceforth, we shall assume that the model to be dealt with is of the generalized Markovian type, i.e. that the model is a finite state Markov or semi-Markov process whose states correspond to the various possible combinations of failure events and RM decision events that can occur. This paper will emphasize discrete parameter models. Similar analyses hold for continuous parameter models.

When generalized Markovian models are used for performance evaluation of realistically complex

systems, a dimensionality problem arises. Complex fault-tolerant systems tend to require many states for their accurate characterization. Furthermore, the operating time (or mission time) for such systems tends to be long relative to the operating cycle time of the RM system. Therefore, the operating times of interest are such that the model must be propagated for many RM cycle times. A further dimensionality problem is engendered by the fact that the system performance may be a function of the entire history of failure and RM decision events. These factors all combine to produce an explosion of the memory size and the number of computations required to evaluate the system performance. Unfortunately, the simplifications that are possible by using steady state analysis of such models are not applicable because the operating time of a fault-tolerant system tends to be only a small fraction of the mean time between failure events. Therefore, the transient behavior of the model is of interest while the steady state behavior is not.

In this paper, we discuss some techniques that are currently under development that lead to approximate results for performance evaluation. First, we discuss a method for discrete parameter Markovian models of fault-tolerant systems that involves the introduction of a "performance transform." By approximating the behavior of the transform, it is possible to generate approximate results for the probability mass function of the random performance value. A means for implementing this approximation is suggested which makes use of an alternative evaluation of the expected value of the performance. Subsequently, a method for continuous parameter models is briefly discussed which exploits the typical separation of time scales between the failure event history and the RM decision history.

2. PERFORMANCE TRANSFORM METHOD

The behavior of many fault-tolerant system designs can be captured by a finite state Markov process with discrete time parameter. The states of such a model represent the various operational states of the fault-tolerant system. They are characterized by the operational status of each of the components and by the status of each of the automatic fault diagnosis tests. For example, a typical state in a model for a fault-tolerant inertial measurement unit would be characterized by the gyros and accelerometers which were still working, those that had already failed, and those that had been eliminated from use by the RM function (note that the latter two sets need NOT be identical) plus the status of all of the fault detection and isolation tests which the RM logic uses. If it can be assumed that the time of failure for each component is exponentially distributed (and hence is generated by a memoryless process) and that each fault diagnostics test operates only on instantaneous data (and is therefore also memoryless), then the various combinations of failure events and test outcomes can be formed which represent transitions of state for the system. If the probabilities of these transitions can be derived, then the state definitions and the transition probabilities taken together constitute a Markov model for the evolution of the system configuration. These models have been used extensively in recent years for the calculation of the reliability of fault-tolerant systems [5,6,7,8].

When the operational state of the system is such that fewer than the nominal number of components are being used or such that some of the components in use are no longer operating normally, then the system performance is degraded. Depending upon the history of such non-nominal conditions, the overall performance of the system in executing its task will also suffer. Let s_k be the integer index of the state occupied at time step k by a discrete parameter Markov model of the system behavior. Assume that $J_k(s_k)$ is the contribution to the overall system performance of occupying state s_k at time step k and that these contributions are cumulative so that the overall system performance is given by:

$$\text{Cost} = \sum_{k=1}^{k_m} J_k(s_k)$$

Clearly, this overall performance value will be a function of the time history of the operational state (or OSH, for Operational State History) and, because each OSH is a sample function of a random process, the performance value will be a random variable. It is possible to compute the probability of occurrence of each and every OSH from the single-step transition probability matrix P of the Markov model and the initial state probability vector π_0, which is usually known and frequently consists of unity for the probability of initially occupying a state characterized by all normal components and zeroes for all the other initial state probabilities. Once the probability of each OSH is known, the entire probability mass function (pmf) of the performance value can be constructed, and the problem is solved.

Unfortunately, the number of OSHs expands very rapidly with elapsed time. If the model consists of S states which form a single communicating class, then the number of distinct OSHs may be as large as S^k where k is elapsed time since the mission began. As was discussed in the Introduction, the elapsed times of interest are frequently large relative to the RM cycle time and S itself is frequently large. As a result, the number of distinct OSHs becomes unmanageably large.

Fault-tolerant systems frequently have the property that component repair is not feasible during a mission and hence need not be considered. In this case, the system configuration can only degrade due to failures or incorrect RM decisions. Also, all fault-tolerant system models include a state that represents configurations which are so degraded that they are unacceptable. This state is the system loss (SL) state, and it is a trapping state when repair is not possible. These circumstances lead to a situation where the number of distinct OSHs that a system can exhibit is not exponential in the number of states. It is sometimes possible to show that the number of distinct OSHs is bounded by a linear function of time. Nonetheless, even in the latter case, the number of OSHs quickly grows to a value that is beyond the memory capability of even large mainframe computers. This motivates the search for approximate methods to compute the statistics of the system performance. We shall now present such a method.

Consider a finite state Markov model of a fault-tolerant system comprising N states, one of which, namely s_N, is the SL trapping state. Associated with the occupancy of each state for a single time step is an integer-valued performance measure. The assumption of integral values here is not restrictive because a general performance

measure can be resolved to the integers by discretizing its value. At this point, we shall also assume that the performance values are time-invariant. If they are time-varying, the algebra becomes considerably more cumbersome, but the results cited below hold except where the assumption of time-invariance is explicitly mentioned. If $J(s_k)$ again represents the performance value incurred by occupancy of state s at time k, we have that:

$$Perf. = \sum_{k=1}^{k_m} J(s_k)$$

where k_m is the length of the mission expressed in number of time steps. This performance value is random because the OSH followed by the system is random. Clearly, if we can calculate the probability of each OSH that the system can follow, then the characterization of the pmf of the system performance value will be complete.

A typical OSH over k time steps takes the form:

$$\{j, s_1, \cdots, i\}$$

which is a list of the states occupied by the system at each of the k time steps. Here, the system initially occupies state j and it occupies state i at the k-th time step. Suppose there are $t_{ij}(k)$ such OSHs, all beginning in state j and ending in state i at th k-th time step but traversing many different states in between. For the l-th such OSH, let its probability be given by $p_{ij}(l,k)$ and the accumulated value of performance be denoted $J_{ij}(l,k)$. We define the performance transform or v-transform for this OSH as:

$$m_{ij}(v,k) \triangleq \sum_{l=1}^{t_{ij}(k)} p_{ij}(l,k)\, v^{J_{ij}(l,k)}$$

The v-transform is a compact way of representing the complete statistical characterization of the performance of the system. Among its properties are the following. If we set v to unity in the v-transform, we obtain:

$$\sum_{l=1}^{t_{ij}(k)} p_{ij}(l,k)$$

which is the probability of reaching state i from state j in k time steps, i.e. the multistep transition probability from state j to state i. If we differentiate the v-transform with respect to v and then set v to unity in the result, we obtain:

$$\sum_{l=1}^{t_{ij}(k)} p_{ij}(l,k)\, J_{ij}(l,k)$$

which is the expected value of the performance after k time steps. This moment-generating property of the v-transform extends to all higher moments of the performance value as well.

Because the performance values associated with occupancy of each state are integer-valued, the exponents in the v-transform are integers. Therefore, the v-transform is always a polynomial in v. The v-transform representation of the behavior of the performance value can therefore be made even more compact by combining terms in the polynomials. This procedure effectively merges OSHs whose beginning and ending states are the same and whose cumulative performance values are identical. The properties cited above for the v-transform remain in force after this combination of terms.

The matrix of v-transforms for all starting and ending states is denoted $M(v,\kappa)$. Its propagation in time is governed by the difference equation:

$$M(v, k+1) = V_k(v)\, M(v, k)$$

where $V_k(v)$ is the single-step v-transform update matrix effective at time step k. $V_k(v)$ is constructed from P by multiplying each row of P by v raised to the power of the performance incurred by occupancy of the corresponding state for one tiem step at time k. If these performance values are time-invariant, then $V_k(v)$ reduces to V(v) and the difference equation becomes:

$$M(v, k+1) = V(v)\, M(v, k)$$

The combination of terms described earlier can be applied at each time step to reduce somewhat the number of terms in the polynomials comprising $M(v,k)$. Note, however, that the problem of keeping track of a large number of OSHs has not been eliminated but merely converted into the problem of keeping track of a large number of polynomial terms.

By successively applying the difference equation, we can generate the v-transform matrix $M(v,k_m)$. The v-transform of the performance of the system assuming it started in state j and did NOT reach system loss during the mission is then given by:

$$W_j(v, k_m) = \sum_{i=1}^{N-1} m_{ij}(v, k_m)$$

SInce it is frequently the case that the system is known to begin the mission with all components operating and no fault detection alarms, it is often true than that the v-transform of the system performance over the mission is given by $W_1(v,k_m)$. This v-transform completely represents the pmf of the system performance, which was the desired result. However, it still suffers from the memory difficulties associated with keeping track of a large number of polynomial terms in generating it. An approximation will now be discussed that circumvents this difficulty.

Assuming once again that the performance values are time-invariant, let r be a row vector of the N values of performance incurred by occupying each of the N states for one time step. Let R(k) be the row vector of expected performance after k time steps starting from each of the N states of the model. Then, the theory of Markov processes with rewards [10] yields the following result:

$$R(k) = r \sum_{n=1}^{k} P^n$$

Because state N is the SL trapping state, the elements of R(k) all tend toward a steady state

asymptote which is linear with a slope of r_N. Consider this value for a moment. It is the performance value incurred for occupancy of the SL state for a single time step. Note, however, that to the system designer, the fact that the system has reached the system loss state means that the system is no longer capable of operating. Therefore, its "performance" upon reaching this level of degradation is irrelevant. Hence, the value chosen for r_N is irrelevant except to the behavior of R(k). In light of this fact, we choose r_N equal to zero to avoid a steady state increase in the values of R(k).

Let us consider again the interpretation of R(k). The elements of R(k) are the expected values of the total accumulated performance over k time steps starting from each of the model states at time 0. Since the system usually starts from state 1, let $R_1(k)$ be denoted $\bar{J}(k)$. This is the expected performance over k time steps for ALL OSHs beginning in state 1, including those which end in state N, the SL trapping state. Note again, however, that OSHs ending in the SL state are not of interest in performance evaluation (except in the computation of the system unreliability). Therefore, $\bar{J}(k)$ can be decomposed into two parts: the portion $\bar{J}_1(k)$ which is the expected performance for those OSHs not ending in the SL state and therefore of interest, and the portion $\bar{J}_{c1}(k)$ which is the expected performance accumulated by those OSHs ending in the SL state and therefore not of interest. Figure 1 illustrates the relationship between these three quantities for a typical example. Note that the mission time k_m is typically short relative to the time at which the expected performance behavior approaches steady state.

With r_N set to zero, it is a relatively easy matter to generate the elements of R(k) for any k and, in particular, to generate $R(k_m)$. This can be done using modal decomposition [9] or any other numerically well-behaved algorithm. $R(k_m)$ can then be used in the following approximation scheme. Note that $R_i(k_m)$ is an upper bound for the expected performance accumulated over k_m time steps beginning from state i and is therefore also an upper bound for the expected performance to be accumulated over $n<k_m$ time steps beginning from state i. Consider a time step k at which we have generated the v-transform matrix M(v,k) whose (i,j)-th element is $m_{ij}(v,k)$ which in turn comprises many terms of the form Av^b where we have assumed that terms with like exponents have already been combined. The approximation we shall use is produced by neglecting all such terms in $m_{ij}(v,k)$ that are such that:

$$A \cdot [b + R_i(k_m)] < \text{tolerance}$$

This has the effect of discarding all OSHs at time k which are expected to have a small contribution to the statistical properties of the performance over the mission. Note that OSHs that have accumulated only a small performance value up to time k and have a small probability might still be retained by this approximation if it is expected that they will accumulate a large performance value during the remainder of the mission. This makes the approximation much less risky than discarding all OSHs whose contribution to the expected performance at time k is small without regard to what their future contribution might be.

In the next Section, a rule of thumb is suggested for setting the tolerance value appearing in the approximation. Note that larger tolerances result in more discarded terms and hence less computational effort and memory burden at a cost of less accuracy. This tradeoff is also examined briefly in the next Section.

3. Results

In this Section, we briefly summarize some numerical results for a 50-state model of a fault-tolerant system. The overall system is assumed to comprise an actuator subsystem and a sensor subsystem. These two subsystems are identical in their redundant architecture and their RM logic but are completely independent otherwise. The Markov model for one subsystem is shown in Figure 2 where D represents a correct detection of a failure, D represents a "missed" detection, D represents a false detection, I represents the isolation of a failure following a detection, I represents no isolation following a detection, and I represents the isolation of the wrong component following a detection. Table 1 lists the values of the conditional probabilities of these events for each time step that were assumed. The actuator subsystem was assumed to consist of components whose mean time to failure was 25 hours. The sensor subsystem components were assumed to have a mean time to failure of 100 hours. The time step, which corresponds in such models to the time between successive failure detection tests, was assumed to be 1 second. The performance associated with occupancy of each of the states of the model was based in the case of the sensors upon the achievable accuracy of the estimation of a three-dimensional quantity measured by the sensor array. A failed sensor was assumed to produce a measurement with an additional error of 3 relative to a good sensor where is the standard deviation of the random error in the measurement from one sensor. The actuator performance values were scaled up from the sensor performance values to reflect the increased importance to a control system of the actuators. Details on the model construction can be found in [9].

When the two independent models are combined, the overall system model consists of 49 operational states plus a SL state for a total of 50 states. Of course, in this particular case there is no need to combine the subsystem models into an overall model in light of their independence. However, we do so here in order to demonstrate the applicability of our method to large models, which are typical in the field of fault-tolerant system performance evaluation.

The results described here were generated on a modified Hewlett-Packard 9826U microcomputer. The major limitation was the limited amount of memory available for use. As a result, results could only be generated for the 50-state model up to 111 time steps when the tolerance was very small. It should be noted, however, that in 111 time steps as many as 30,000 OSHs must be kept track of even after merging those that have the same ending states and same performance values. A computer with virtual memory allows for much longer runs. Nevertheless, the characteristics exhibited by the results after 111 time steps are sufficient to illustrate the insight that can be gained from a performance evaluation tool.

Figures 3, 4 and 5 illustrate the effect of the tolerance level in the approximation on the results. Each is a plot of the computed performance pmf after 150 time steps for a 7-state model which is similar in scope to the 8-state

model for each of the subsystems described above. The probability axis (vertical) on each plot is logarithmic. The point at which the tolerance begins to have a profound effect on the results is at a tolerance level between 10^{-3} and 10^{-2}. The total expected performance for this system at 150 time steps (i.e. the expected value of the performance accumulated by OSHs up to this time point without regard to whether or not they have reached the SL state) is 62.7. Hence, the performance pmf results begin to break down when the tolerance reaches a value approximately 4 decades below the total expected performance for the mission (which can be calculated easily by the Markov process with rewards result). In all of the results generated in this study so far, this has been a good rule of thumb: Set the tolerance at least 4 decades below the total expected performance to avoid inaccurate results for the approximate performance pmf.

Returning to the 50-state model, the value of its expected performance at 350 time steps is 4560. By the rule of thumb above then, the tolerance should be set no larger than 0.4 to generate reasonably accurate results for the performance pmf. Figure 6 is the performance pmf for the 50-state model after 350 time steps using a tolerance of 0.1. Note that this value of the tolerance has allowed propagation of the v-transform matrix to a number of steps at which as many as 100,000 different OSHs would have to be kept track of were it not for the approximation.

Further results for these models are given in [9], which also uses the modal decomposition of the result form the theory of Markov processes with rewards to generate a reduced order model that approximates the performance behavior of the 50-state model.

4. Brief Discussion of Other Work

A related research effort is currently exploring another avenue toward the generation of approximate performance evaluation results for fault-tolerant systems. This work exploits the separation in time scales of the failure behavior of components and the behavior of the tests used to detect and isolate those failures. In particular, a well-designed fault-tolerant system includes a failure detection mechanism which detects and isolates failures very quickly. On the other hand, the failures themselves tend to occur only rarely and are therefore considerably spread out in time. If a finite state Markov model or semi-Markov model is constructed to represent the behavior of the fault-tolerant system, then it oftentimes naturally decomposes into classes of states. The states within each class are such that the transitions between them are frequent with small holding times as determined by the failure detection decision processes. Meanwhile, the transitions between the classes are governed by the failure processes and are therefore much slower and less frequent. Once the system model is decomposed in this fashion, it is almost in a form to which some recent results from the theory of Markovian processes with rare events can be applied. However, for fault-tolerant system models, there remain a few difficulties. Overcoming these difficulties is the subject of our current efforts.

5. Conclusion

In this paper, we have briefly described some approximate techniques for evaluating the statistical properties of the performance of fault-tolerant control systems. As such systems come into wider use, the availability of design tools based upon performance evaluation techniques will be increasingly important. The method described here circumvents the difficulty of dimensionality encountered by straightforward combinatorial and Markovian techniques by introducing the v-transform representation and then using it to suggest an approximate simplification which increases considerably the efficiency of the performance evaluation algorithm for large-scale models without sacrificing significant accuracy. Some numerical results illustrate a rule of thumb for using the algorithm and illustrate some of the useful performance properties that result.

Acknowledgment

This work was supported in part by NASA Langley Research Center under Grant No. NAG1-126 and in part by the Air Force Office of Scientific Research under Grant No. AFOSR-84-0160.

References

[1] M.L. Shooman, Probabilistic Reliability: An Engineering Approach, McGraw-Hill, 1968.

[2] B.K. Walker, "Performance Evaluation of Systems That Include Fault Diagnostics," Proc. of Joint Auto. Control Conf., Charlottesburg, VA, June 1981.

[3] R.H. Luppold, "Reliability and Availability Models for Fault-Tolerant Systems," S.M. thesis, Dept. of Aero. and Astro., M.I.T., August 1983.

[4] R.H. Luppold, E. Gai, and B.K. Walker, "Effects of Redundancy Management on Reliability Modelling," Proc. of 3rd American Control Conf., San Diego, June 1984.

[5] B.K. Walker and E. Gai, "Fault Detection Threshold Determination Technique Using Markov Theory," J. of Guidance and Control, 2:4:313-319, July-August 1979.

[6] E. Gai, J.V. Harrison, and R.H. Luppold, "Reliability Analysis of a Dual-Redundant Engine Controller," SAE technical paper 811077, October 1981.

[7] J.V. Harrison, K.C. Daly, and E. Gai, "Reliability and Accuracy Prediction for a Redundant Strapdown Navigator," J. of Guidance and Control, 4:5:523-529, September-October 1981.

[8] R.S Schabowsky, E. Gai, B.K. Walker, J.H. Lala, and P. Motyka, "Evaluation Methodologies for an Advanced Information Processing System," Proc. of 6th Digital Avionics Systems Conf., Baltimore, December 1984.

[9] D.K. Gerber, "Performance Evaluation of Fault-Tolerant Systems Using Transient Markov Models," S.M. thesis, Dept. of Elect. Eng. and Computer Sci., M.I.T., June 1985.

[10] R.A. Howard, Dynamic Programming and Markov Processes MIT Press, 1960.

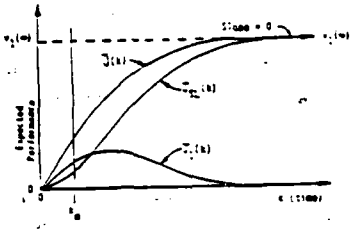


Figure 1.

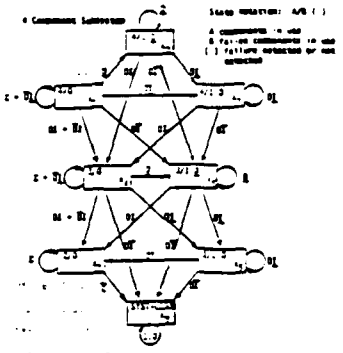


Figure 2.

	Event Probability for State:					
	4/0	4/1 D	4/1 S	3/0	3/1 D	3/1 S
P(F) =	.99	1.0	.95	.98	1.0	.92
P(S) =	.001	N/A	N/A	.005	N/A	N/A
P(1DF) =	.75	.65	.75	.65	.60	.65
P(2DF) =	.01	.05	.01	.01	.02	.10
P(1SF) =	.24	.30	.24	.25	.38	.25
P(1S) =	.005	N/A	N/A	.025	N/A	N/A

Table 1.

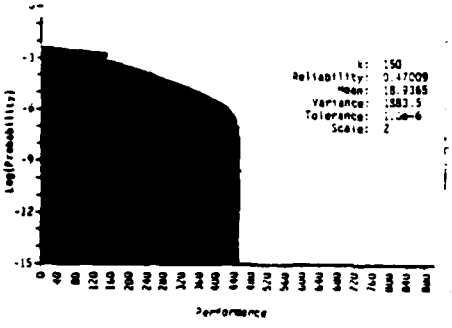


Figure 3.

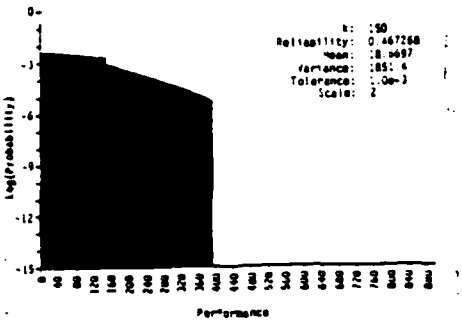


Figure 4.

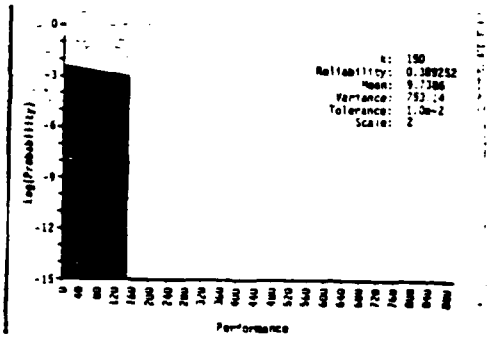


Figure 5.

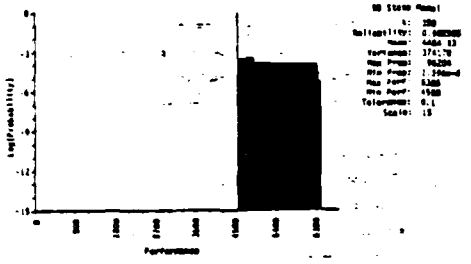


Figure 6.

END

DTIC

7-86